MAT-8067US

PATENT

#4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Y. Murakawa : Art Unit: 2131
Serial No.: 09/729,262 : Examiner:
Filed: December 1, 2000 : Box Missing Parts
FOR: METHOD OF VIRTUAL PRIVATE NETWORK COMMUNICATION IN SECURITY GATEWAY APPARATUS AND SECURITY GATEWAY APPARATUS USING THE SAME : :

CLAIM TO RIGHT OF PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231
SIR:

Pursuant to 35 U.S.C. 119, Applicant's claim to the benefit of filing of prior Japanese Patent Application No. 11-344500, filed December 3, 1999, is hereby confirmed.

A certified copy of the above-referenced application is enclosed.

Respectfully submitted,

Lawrence E. Ashery, Reg. No. 34,515
Attorney for Applicant

LEA/dlm

Encl.: (1) certified priority document

Dated: April 5, 2001

Suite 301, One Westlakes, Berwyn
P.O. Box 980
Valley Forge, PA 19482
(610) 407-0700

The Assistant Commissioner for Patents is hereby authorized to charge payment to Deposit Account No. 18-0350 of any fees associated with this communication.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231 on:

April 5, 2001

Lawrence E. Ashery

MAT-8067US

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年１２月 ３日

出 願 番 号
Application Number: 平成１１年特許願第３４４５００号

出 願 人
Applicant (s): 松下電器産業株式会社

２０００年１１月１０日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３０９４１８１

【書類名】　特許願

【整理番号】　2913011174

【提出日】　平成11年12月 3日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/28

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　村川　泰

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　　不要

【書類名】　明細書

【発明の名称】　セキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法

【特許請求の範囲】

【請求項１】公衆回線などから構成されるＷＡＮとＬＡＮとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法であって、ダイヤルアップ接続でＷＡＮに接続した外部のＰＣに対してＩＰｓｅｃプロトコルによりＶＰＮを実現する際、ＩＰｓｅｃ通信に先立つＩＫＥ通信時に、ＤＨＣＰ通信オプションをＩＫＥデータに統合し、トンネリングされたＩＰパケットにおけるＩＰｓｅｃ処理される送信元ＩＰアドレスの指定を実現するセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法。

【請求項２】ＩＫＥ通信時に、セキュリティ・ゲートウェイ装置配下のＬＡＮと同じセグメントのＩＰアドレス／サブネットマスクアドレスをダイヤルアップ接続からＬＡＮにアクセスする前記外部のＰＣに割り当て、前記外部のＰＣを仮想的にＬＡＮ環境下に置いたＶＰＮ通信を実現する請求項１に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法。

【請求項３】ＮＡＴ技術を組み合わせて前記外部のＰＣにＬＡＮ配下で使用しているプライベートＩＰアドレスをＩＫＥ通信時に付与し、プライベートＩＰアドレスで構築されたＬＡＮ環境への前記外部のＰＣからのアクセスが可能なＶＰＮ通信を実現するセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数のＰＣを接続したＬＡＮと公衆回線などのＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）とを集線・変換処理を行うことにより接続するセキュリティ・ゲートウェイ装置で構成されるネットワーク環境において、公衆回線にダイヤルアップ接続した外部のＰＣがＷＡＮを介してセキュリティ・ゲートウェイ装置とＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ、仮想専用網）通信を行うためのセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法に関するものである。

【０００２】

【従来の技術】

近年、企業のみならず家庭に至るまで複数台のＰＣが導入され、インターネットへの接続が進んでいる。複数台のＰＣで構成されるＬＡＮをインターネットに接続する場合、ＬＡＮとＷＡＮを接続するゲートウェイ装置が必要になる。また、ＬＡＮの外部のＰＣからＬＡＮ配下の端末にアクセスするには、まず契約しているプロバイダにダイヤルアップ接続し、ＷＡＮ経由でＬＡＮ配下の端末（例えばＰＣ）にアクセスすることになる。

【０００３】

しかし、ＷＡＮを流れるパケットは基本的に安全性が確保されておらず、パケットを盗聴されると、第三者に通信内容を悪用される恐れがある。通信内容の秘匿性と外部からの不正アクセスを防止するためには、ＷＡＮとＬＡＮを接続するセキュリティ・ゲートウェイ装置が必要となり、ダイヤルアップ接続するＰＣにもセキュリティのための通信プロトコルスタックが実装されてないといけない。そして、外部からアクセスするＰＣ（外部のＰＣ）とセキュリティ・ゲートウェイ装置の間でＶＰＮ通信を行うことで、ＷＡＮ上で仮想的な専用線環境が実現できる。現在、ＶＰＮ通信のための代表的な通信プロトコルとして実装されているのはＩＰｓｅｃ（Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ｔｈｅ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）である。

【０００４】

以下に、ＩＰｓｅｃを利用したＶＰＮ通信の概要を説明する。まず図４を参照しながら説明する。図４はＷＡＮを含む一般的なネットワークシステムを示す構成図である。

【０００５】

図４において、１０１はプロバイダにダイヤルアップ接続した外部のＰＣ、１０２はＷＡＮ、１０３はＷＡＮ１０２と後述のＬＡＮ１０４を接続して集線・変換処理を行うセキュリティ・ゲートウェイ、１０４はセキュリティ・ゲートウェイ１０３配下のＬＡＮ、１０５はＬＡＮ１０４上のサーバ端末、１０６、１０７はＬＡＮ１０４上のクライアントＰＣ、１０８はＰＣ１０１とセキュリティ・ゲ

ートウェイ１０３との間でＩＰｓｅｃ通信を行うために確立されたＶＰＮである。

【０００６】

ダイヤルアップ接続したＰＣ１０１がＬＡＮ１０４上の端末にアクセスする場合、セキュリティ・ゲートウェイ１０３との間でＶＰＮ１０８を確立し、ＷＡＮ１０２上で仮想的な専用線環境を実現する。こうしてＷＡＮ１０２上で通信内容を盗聴・改竄できないようにし、ＬＡＮ１０４配下の端末と通信を行う。

【０００７】

次に、ＩＰｓｅｃ通信を行うために必要な通信内容の概要について図５を用いて解説する。図５はＷＡＮによる接続を示すＷＡＮ接続図である。

【０００８】

図５において、ＰＣ１０１、ＷＡＮ１０２、セキュリティ・ゲートウェイ１０３は図４と同様のものである。

【０００９】

ＰＣ１０１とセキュリティ・ゲートウェイ１０３との２点間でＩＰｓｅｃ通信を行う場合、データの秘匿性、コネクションレスな完全性（相手との論理的な通信路を構築せず、データの改ざんを防止すること）、改ざん防止などを保証するための暗号アルゴリズム、認証アルゴリズムに用いる鍵情報を両者がＩＰｓｅｃ通信を行う前に共有できてないといけない。両者で鍵情報を共有させる方法として、事前に両者で鍵情報を手動で設定する方法と、ＩＫＥ（Ｉｎｔｅｒｎｅｔ Ｋｅｙ Ｅｘｃｈａｎｇｅ）プロトコルを用いて自動設定する方法の２通りがある。ここでは、現実的な方法であるＩＫＥプロトコルによる自動鍵情報交換方式のみを適用する。

【００１０】

次に、図６を用いてＩＰｓｅｃ通信について説明する。図６はＩＰｓｅｃ通信開始のためのセキュリティ・ゲートウェイ１０３の動作を示すフローチャートである。

【００１１】

ＩＰｓｅｃ通信を行うためには、２点間で双方向に論理的なコネクションＳＡ

（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）を確立しなければならない。そのためにＩＫＥ通信は２つのフェーズに分かれていて、フェーズ１において安全なＩＫＥ通信を行うためのＩＫＥ－ＳＡを確立しようとし（Ｓ１１、Ｓ１２）、それに成功したら、フェーズ２において、ＩＰｓｅｃ通信するための鍵情報などのセキュリティ情報を交換する（Ｓ１３）。フェーズ２でＩＰｓｅｃ－ＳＡを確立することができれば（Ｓ１４）ＩＫＥ通信を終了し、ＩＰｓｅｃ通信が開始する（Ｓ１５）。ステップＳ１３のＩＫＥ（フェーズ２）通信においてＩＰｓｅｃ通信を行うために２点間で交換される情報を（表１）に示す。

【００１２】

【表１】

項　目	詳　　細
セキュリティ・プロトコル	ESP/AH
IPsec通信モード	トンネルモード/トランスポートモード
暗号アルゴリズム	ESPの場合必須
暗号鍵	－
認証アルゴリズム	AHの場合必須、ESPでも選択可
認証鍵	－
SAの寿命形式	データ量(バイト)／時間(量)
SAの寿命	－

【００１３】

但し動作モード（ＩＰｓｅｃ通信モード）については、セキュリティ・ゲートウェイ１０３はトンネルモード（ＩＰパケット全体をカプセリングする）でしか動作できないので、ここでは、ＩＰｓｅｃの動作モードはトンネルモードのみを想定する。

【００１４】

図７はトンネルモードのＩＰｓｅｃ通信の概要を示す説明図である。

【００１５】

図７において、ＰＣ１０１、セキュリティ・ゲートウェイ１０３、ＬＡＮ１０４、クライアントＰＣ１０６、ＶＰＮ１０８は図４と同様のものである。１００はＩＰパケットである。

【００１６】

図７において、ＰＣ１０１、セキュリティ・ゲートウェイ１０３、クライアントＰＣ１０６のＩＰアドレスをそれぞれＡ、Ｂ、Ｃとする（Ａはプロバイダによってｐｃ１０１に付与されたＩＰアドレス）。ＬＡＮ１０４上のクライアントＰＣ１０６からＶＰＮ１０８を介してコネクションの張られたＰＣ１０１にＩＰパケットを送信する場合、まずクライアントＰＣ１０６において、送信元ＩＰアドレスがＣ、宛先ＩＰアドレスがＡのＩＰパケット１００が作成され、送信される。セキュリティ・ゲートウェイ１０３がこのパケット１００を受信し、ＶＰＮ１０８を張られたＰＣ１０１宛てのパケットであることを識別すると、ＩＫＥ通信による交換した情報に基づいてＩＰパケット１００をカプセリングする。元のＩＰアドレスの外側に、送信元ＩＰアドレスＢ、宛先ＩＰアドレスＡのＩＰヘッダが付加される。このとき交換した情報に基づいてカプセリングされたＩＰパケットへの認証情報の付加、暗号化が行われる。ＶＰＮ１０８を介してカプセリングされたパケットを受信したＰＣ１０１は、交換した情報に基づいてカプセリングされた元のＩＰパケット１００を取り出し、処理する。

【００１７】

【発明が解決しようとする課題】

しかしながら、上記従来のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法では、ＷＡＮ１０２上でのデータの安全性は確保できているが、あくまで外部ネットワークからのアクセスと判断されるため、ＬＡＮ１０４配下のクライアントＰＣ１０６の情報にアクセスするために、ＬＡＮ１０４配下のクライアントＰＣ１０６に設定（アクセス許可／不許可を示すセキュリティ・ポリシーの設定、例えば許可するＩＰアドレスと不許可となるプロトコル・サービスなど）が必要になり、その設定のために別の安全性の問題が生じる可能性があり、ＬＡＮ１０４がプライベートＩＰアドレスで構成されたネットワークの場合、その設定

は特に困難になるという問題点を有していた。

【００１８】

このセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法では、ＷＡＮを介して外部からアクセスするＰＣを仮想的にＬＡＮ配下の端末として通信可能にすることが要求されている。

【００１９】

本発明は、この要求を満たすため、ＷＡＮを介して外部からアクセスするＰＣを仮想的にＬＡＮ配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法を提供することを目的とする。

【００２０】

【課題を解決するための手段】

この課題を解決するために本発明のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法は、公衆回線などから構成されるＷＡＮとＬＡＮとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法であって、ダイヤルアップ接続でＷＡＮに接続した外部のＰＣに対してＩＰｓｅｃプロトコルによりＶＰＮを実現する際、ＩＰｓｅｃ通信に先立つＩＫＥ通信時に、ＤＨＣＰ通信オプションをＩＫＥデータに統合し、トンネリングされたＩＰパケットにおけるＩＰｓｅｃ処理される送信元ＩＰアドレスの指定を実現する構成を備えている。

【００２１】

これにより、ＷＡＮを介して外部からアクセスするＰＣを仮想的にＬＡＮ配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法が得られる。

【００２２】

【発明の実施の形態】

本発明の請求項１に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法は、公衆回線などから構成されるＷＡＮとＬＡＮとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法であって、ダイヤルアップ接続でＷＡＮに接続した外部のＰＣに対してＩＰｓｅｃプロ

トコルによりＶＰＮを実現する際、ＩＰｓｅｃ通信に先立つＩＫＥ通信時に、ＤＨＣＰ通信オプションをＩＫＥデータに統合し、トンネリングされたＩＰパケットにおけるＩＰｓｅｃ処理される送信元ＩＰアドレスの指定を実現することとしたものである。

【００２３】

この構成により、セキュリティ・ゲートウェイ装置は、ダイアルアップ接続した外部のＰＣとＩＰｓｅｃ通信する際、そのＰＣの最終的な宛先ＩＰアドレスを制御可能にし、ＬＡＮ配下の端末への設定を不要とし、安全性が確保されるという作用を有する。

【００２４】

請求項２に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法は、請求項１に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法において、ＩＫＥ通信時に、セキュリティ・ゲートウェイ装置配下のＬＡＮと同じセグメントのＩＰアドレス／サブネットマスクアドレスをダイヤルアップ接続からＬＡＮにアクセスする外部のＰＣに割り当て、外部のＰＣを仮想的にＬＡＮ環境下に置いたＶＰＮ通信を実現することとしたものである。

【００２５】

この構成により、ＶＰＮを確立した外部のＰＣがＬＡＮ環境内にあるように仮想的にみなせる作用を有する。

【００２６】

請求項３に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法は、請求項１に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法において、ＮＡＴ技術を組み合わせて外部のＰＣにＬＡＮ配下で使用しているプライベートＩＰアドレスをＩＫＥ通信時に付与し、プライベートＩＰアドレスで構築されたＬＡＮ環境への外部のＰＣからのアクセスが可能なＶＰＮ通信を実現することとしたものである。

【００２７】

この構成により、プライベートＩＰアドレスで構成されたＬＡＮ環境に、安全性を確保したまま外部のＰＣからのアクセスを可能にするという作用を有する。

【００２８】

以下、本発明の実施の形態について、図１～図３を用いて説明する。

【００２９】

（実施の形態１）

図３は、本発明の実施の形態１によるセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法において用いるＩＫＥ通信データフォーマットを示すフォーマット図である。

【００３０】

図３に示す通り、ＩＫＥ通信はＵＤＰ（Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）／ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）を使用して行われる。ＩＫＥデータは、ＩＳＡＫＭＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）ヘッダの後にＩＳＡＫＭＰペイロードが数珠つなぎの形態で続くことで構成される。ＩＫＥ通信は、鍵交換を要求する始動者（イニシエータ、Ｉｎｉｔｉａｔｏｒ）とそれに対して応答する応答者（リスポンダ、Ｒｅｓ－ｐｏｎｄｅｒ）によって行われる。本実施の形態においては、図４において、プロバイダにダイヤルアップしてインターネットに接続したＰＣ１０１がＩｎｉｔｉａｔｏｒとなり、ＬＡＮ１０４上の端末としてのクライアントＰＣ１０６、１０７にアクセスするために、セキュリティ・ゲートウェイ１０３にＩＫＥ通信を開始し、セキュリティ・ゲートウェイ１０３がＲｅｓｐｏｎｄｅｒとしてＩＫＥ通信を行う。（表１）に挙げた項目のうち、暗号鍵と認証鍵は、公開鍵暗号方式を用いてＩｎｉｔｉａｔｏｒとＲｅｓｐｏｎｄｅｒの間で鍵情報が交換されるが、それ以外の項目は、Ｉｎｉｔｉａｔｏｒが提案をし、ＲｅｓｐｏｎｄｅｒがＩｎｉｔｉａｔｏｒの提案の中から最適なものを選択して応答するというサーバ／クライアントモデルで行われる。ＤＨＣＰ（Ｄｙｎａｍｉｃ　Ｈｏｓｔ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）クライアントとしてのＰＣ１０１が取得すべき必須の情報として、ＩＰアドレス、サブネットマスク、ＩＰアドレスの有効期限、ドメイン名がある。これら４つの情報をＩＫＥ通信においてＲｅｓｐｏｎｄｅｒであるセキュリティ・ゲートウェイ１０３が通常のＩＫＥデータでオプショ

ンとして付加する。但し、ＩＰアドレスの有効期限はＩＫＥ通信によって確立されるＳＡの寿命と同じと考えることで省略することができる。またＤＨＣＰもＵＤＰの上位に位置するアプリケーションプロトコルなので、ＩＫＥに組み込んでも再送制御その他の問題は起こらない。

【００３１】

図１は本発明の実施の形態１におけるＩＰｓｅｃ通信の概略を示す説明図である。

【００３２】

図１において、ＰＣ１０１、セキュリティ・ゲートウェイ１０３、ＬＡＮ１０４、クライアントＰＣ１０６、ＶＰＮ１０８は図４と同様のものである。

【００３３】

図１において、ＰＣ１０１、セキュリティ・ゲートウェイ１０３、クライアントＰＣ１０６のＩＰアドレスをそれぞれＡ、Ｂ、Ｃとする（Ａはプロバイダによってｐｃ１０１に付与されたＩＰアドレス）。また、ＩＰｓｅｃ通信に先立つＩＫＥ通信により、セキュリティ・ゲートウェイ１０３は、ＰＣ１０１にＩＰアドレスＤを配布する。ＬＡＮ１０４上のクライアントＰＣ１０６からＶＰＮ１０８を介してコネクションの張られたＰＣ１０１にＩＰパケットを送信する場合、まずクライアントＰＣ１０６において、ＬＡＮ１０４外部でプロバイダによってＰＣ１０１に割り当てられたＩＰアドレスＡを意識することなく、送信元ＩＰアドレスがＣ、宛先ＩＰアドレスがＤのＩＰパケット１０９が作成され、送信される。セキュリティ・ゲートウェイ１０３がこのパケット１０９を受信し、ＶＰＮ１０８を張られたＰＣ１０１宛てのパケットであることを識別すると、ＩＫＥ通信による交換した情報に基づいてＩＰパケット１０９をカプセリングする。元のＩＰアドレスの外側に、送信元ＩＰアドレスＢ、宛先ＩＰアドレスＡのＩＰヘッダが付加される。このとき交換した情報に基づいてカプセリングされたＩＰパケットへの認証情報の付加、暗号化が行われる。ＶＰＮ１０８を介してカプセリングされたパケットを受信したＰＣ１０１は、交換した情報に基づいてカプセリングされた元のＩＰパケット１０９を取り出し、ＩＫＥ通信により取得したサブネットマスク、ドメイン名を元にＩＰパケット１０９を処理する。

【００３４】

図２はセキュリティ・ゲートウェイ１０３がＰＣ１０１にＩＰアドレスＤを配布する手順を示すフローチャートである。

【００３５】

ＩＰｓｅｃ通信を行うためには、２点間で双方向に論理的なコネクションＳＡを確立しなければならない。そのためにＩＫＥ通信は２つのフェーズに分かれていて、フェーズ１において安全なＩＫＥ通信を行うためのＩＫＥ－ＳＡを確立しようとし（Ｓ１、Ｓ２）、それに成功したら、フェーズ２において、ＩＰｓｅｃ通信するための鍵情報などのセキュリティ情報を交換する（Ｓ３）。フェーズ２でＩＰアドレスＤを配布し、ＩＰｓｅｃ－ＳＡを確立することができれば（Ｓ４）ＩＫＥ通信を終了する（Ｓ５）。ステップＳ３のＩＫＥ（フェーズ２）通信においてＩＰｓｅｃ通信を行うために２点間で交換される情報は（表１）に示す通りである。

【００３６】

以上のように本実施の形態によれば、ダイヤルアップ接続でＷＡＮ１０２に接続したＰＣ１０１に対してＩＰｓｅｃプロトコルによりＶＰＮ１０８を実現する際、ＩＰｓｅｃ通信に先立つＩＫＥ通信時に、ＤＨＣＰ通信オプションをＩＫＥデータに統合し、トンネリングされたＩＰパケットにおけるＩＰｓｅｃ処理される送信元ＩＰアドレスの指定（アドレスＣの指定）を実現するようにしたことにより、セキュリティ・ゲートウェイ１０３は、ダイアルアップ接続した外部のＰＣ１０１とＩＰｓｅｃ通信する際、そのＰＣの最終的な宛先ＩＰアドレスＡを制御可能にし、ＬＡＮ１０４配下のクライアント端末１０６への設定を不要とすることができるので、通信内容の盗聴、改竄のおそれが無くなり、安全性を確保することができる。

【００３７】

（実施の形態２）

本発明の実施の形態２によるセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法を図１を用いて説明する。

【００３８】

図１において、ＩＫＥ通信のＲｅｓｐｏｎｄｅｒであるセキュリティ・ゲートウェイ１０３からＩｎｉｔｉａｔｏｒであるＰＣ１０１にＤＨＣＰ情報を配布する際に、セキュリティ・ゲートウェイ１０３配下のＬＡＮ１０４と同じセグメントのＩＰアドレス、サブネットマスクを配布する。ＶＰＮ１０８確立後のＩＰｓｅｃ通信において、ＶＰＮ１０８上を流れるパケット以外は、ＬＡＮ１０４外部から接続するＰＣ１０１も、セキュリティ・ゲートウェイ１０３配下のクライアント端末１０６とネットワークセグメント上区別のない、しかも一意な端末として通信を行う。

【００３９】

以上のように本実施の形態によれば、ＩＫＥ通信時に、セキュリティ・ゲートウェイ１０３配下のＬＡＮ１０４と同じセグメントのＩＰアドレス／サブネットマスクアドレスをダイヤルアップ接続からＬＡＮ１０４にアクセスするＰＣ１０１に割り当て、外部のＰＣ１０１を仮想的にＬＡＮ１０４環境下に置いたＶＰＮ通信を実現するようにしたことにより、ＶＰＮ１０８を確立した外部のＰＣ１０１がＬＡＮ１０４環境内にあるように仮想的にみなすことができるので、安全性を確保したまま外部からＬＡＮ１０４内の端末にアクセスすることができる。

【００４０】

（実施の形態３）

本発明の実施の形態３によるセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法を図１を用いて説明する。

【００４１】

図１において、セキュリティ・ゲートウェイ１０３がＮＡＴ（ Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｏｒ）技術を用い、セキュリティ・ゲートウェイ１０３配下のＬＡＮ１０４をプライベートＩＰアドレスのみで構成していた場合、通常は外部からＬＡＮ１０４上のクライアント端末１０６にはアクセスできないが、ダイヤルアップ接続したＰＣ１０１とセキュリティ・ゲートウェイ１０３がＶＰＮ１０８を確立するためのＩＫＥ通信の中で、セキュリティ・ゲートウェイ１０３配下のＬＡＮ１０４で使用されているセグメントにおける、まだ使用されていないプライベートＩＰアドレスをＩＫＥに組み込んだＤＨＣＰ

オプションによりＰＣ１０１に配布することにより、ＷＡＮ１０２上にあるＶＰＮ１０８上はグローバルＩＰアドレスで通信しながら、ＬＡＮ１０４内、そしてＰＣ１０１の内部では、プライベートＩＰアドレスでネットワークセグメント上区別のない、しかも一意な端末として通信を行うことができる。

【００４２】

以上のように本実施の形態によれば、ＮＡＴ技術を組み合わせて外部のＰＣ１０１にＬＡＮ１０４配下で使用しているプライベートＩＰアドレスをＩＫＥ通信時に付与し、プライベートＩＰアドレスで構築されたＬＡＮ１０４環境への外部からのアクセスが可能なＶＰＮ通信を実現するようにしたことにより、プライベートＩＰアドレスで構成されたＬＡＮ１０４環境に、安全性を確保したまま外部のＰＣ１０１からのアクセスが可能になる。

【００４３】

【発明の効果】

以上説明したように本発明の請求項１に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法によれば、公衆回線などから構成されるＷＡＮとＬＡＮとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法であって、ダイヤルアップ接続でＷＡＮに接続した外部のＰＣに対してＩＰｓｅｃプロトコルによりＶＰＮを実現する際、ＩＰｓｅｃ通信に先立つＩＫＥ通信時に、ＤＨＣＰ通信オプションをＩＫＥデータに統合し、トンネリングされたＩＰパケットにおけるＩＰｓｅｃ処理される送信元ＩＰアドレスの指定を実現することにより、セキュリティ・ゲートウェイ装置は、ダイアルアップ接続した外部のＰＣとＩＰｓｅｃ通信する際、そのＰＣの最終的な宛先ＩＰアドレスを制御可能にし、ＬＡＮ配下の端末への設定を不要とすることができるので、安全性を確保することができるという有利な効果が得られる。

【００４４】

請求項２に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法によれば、請求項１に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法において、ＩＫＥ通信時に、セキュリティ・ゲートウェイ装置配下のＬＡＮと同じセグメントのＩＰアドレス／サブネットマスクアドレスをダイヤルアップ

接続からＬＡＮにアクセスする外部のＰＣに割り当て、外部のＰＣを仮想的にＬＡＮ環境下に置いたＶＰＮ通信を実現することにより、ＶＰＮを確立した外部のＰＣがＬＡＮ環境内にあるように仮想的にみなすことができるので、安全性を確保したまま外部からＬＡＮ内の端末にアクセスすることができるという有利な効果が得られる。

【００４５】

請求項３に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法によれば、請求項１に記載のセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法において、ＮＡＴ技術を組み合わせて外部のＰＣにＬＡＮ配下で使用しているプライベートＩＰアドレスをＩＫＥ通信時に付与し、プライベートＩＰアドレスで構築されたＬＡＮ環境への外部のＰＣからのアクセスが可能なＶＰＮ通信を実現することにより、プライベートＩＰアドレスで構成されたＬＡＮ環境に、安全性を確保したまま外部のＰＣからのアクセスが可能になるという有利な効果が得られる。

【図面の簡単な説明】

【図１】

本発明の実施の形態１におけるＩＰｓｅｃ通信の概略を示す説明図

【図２】

セキュリティ・ゲートウェイが外部のＰＣにＩＰアドレスを配布する手順を示すフローチャート

【図３】

本発明の実施の形態１によるセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法において用いるＩＫＥ通信データフォーマットを示すフォーマット図

【図４】

ＷＡＮを含む一般的なネットワークシステムを示す構成図

【図５】

ＷＡＮによる接続を示すＷＡＮ接続図

【図６】

ＩＰｓｅｃ通信開始のためのセキュリティ・ゲートウェイ装置の動作を示すフ

ローチャート

【図７】

トンネルモードのＩＰｓｅｃ通信の概要を示す説明図

【符号の説明】

１０１　ＰＣ

１０２　ＷＡＮ

１０３　セキュリティ・ゲートウェイ

１０４　ＬＡＮ

１０５　サーバ端末

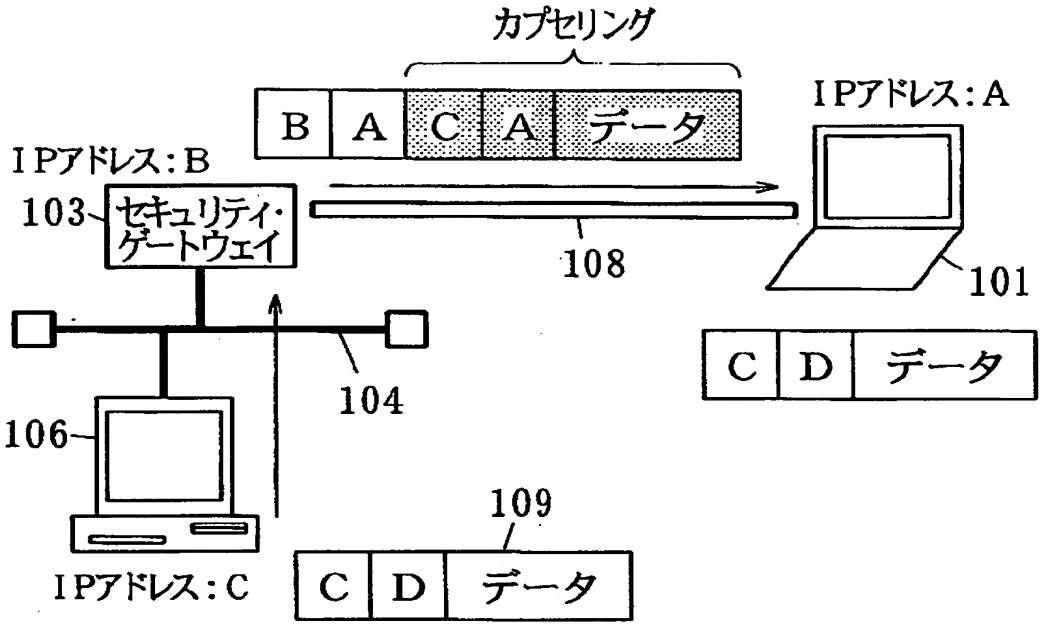
１０６、１０７　クライアント端末（クライアントＰＣ）

１０８　ＶＰＮ

１０９　ＩＰパケット

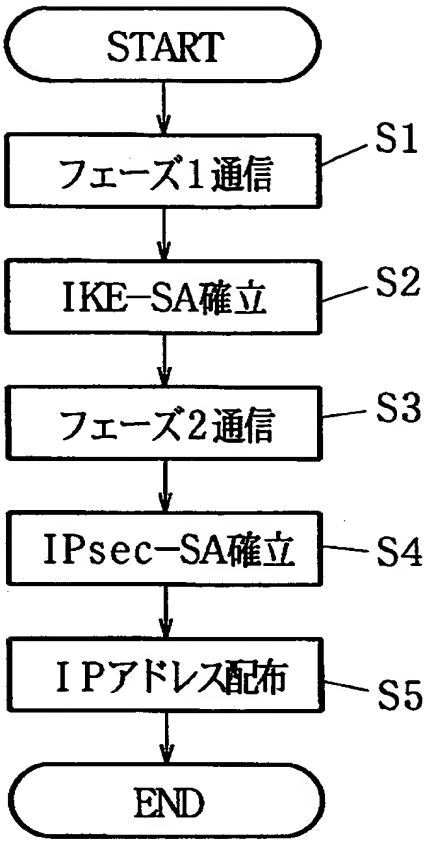
【書類名】　　図面

【図１】

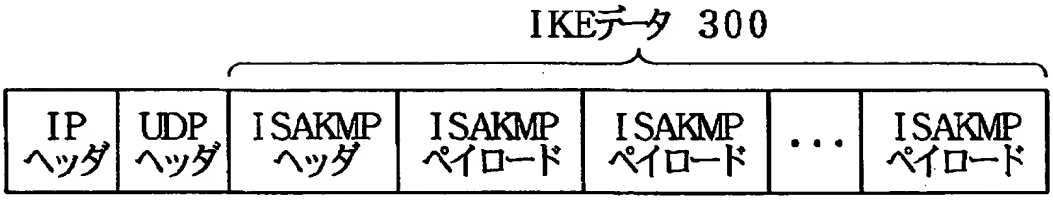


101 PC
103 セキュリティ・ゲートウェイ装置
104 LAN
106 クライアント端末(クライアントPC)
108 VPN
109 IPパケット

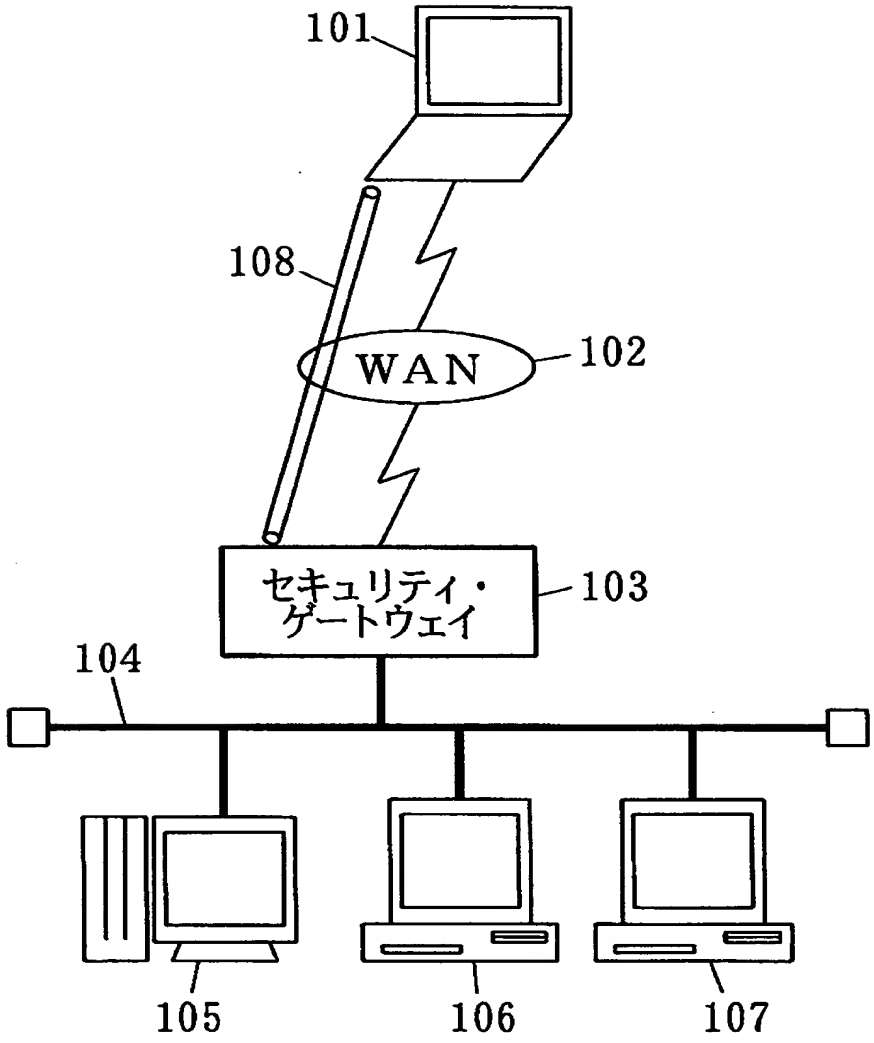
【図２】


START
フェーズ1通信
S1
IKE-SA確立
S2
フェーズ2通信
S3
IPsec-SA確立
S4
ＩＰアドレス配布
S5
END

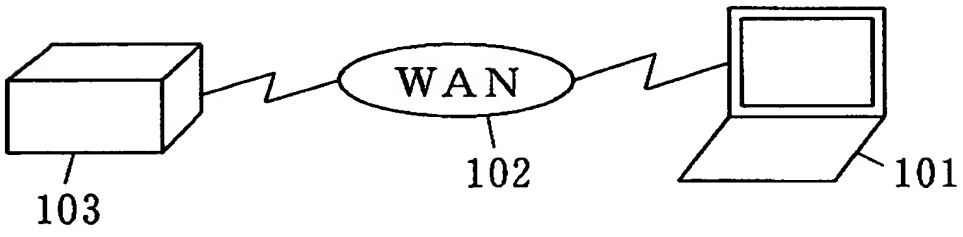
【図３】


IKEデータ 300
IP ヘッダ
UDP ヘッダ
ISAKMP ヘッダ
ISAKMP ペイロード
ISAKMP ペイロード
・・・
ISAKMP ペイロード

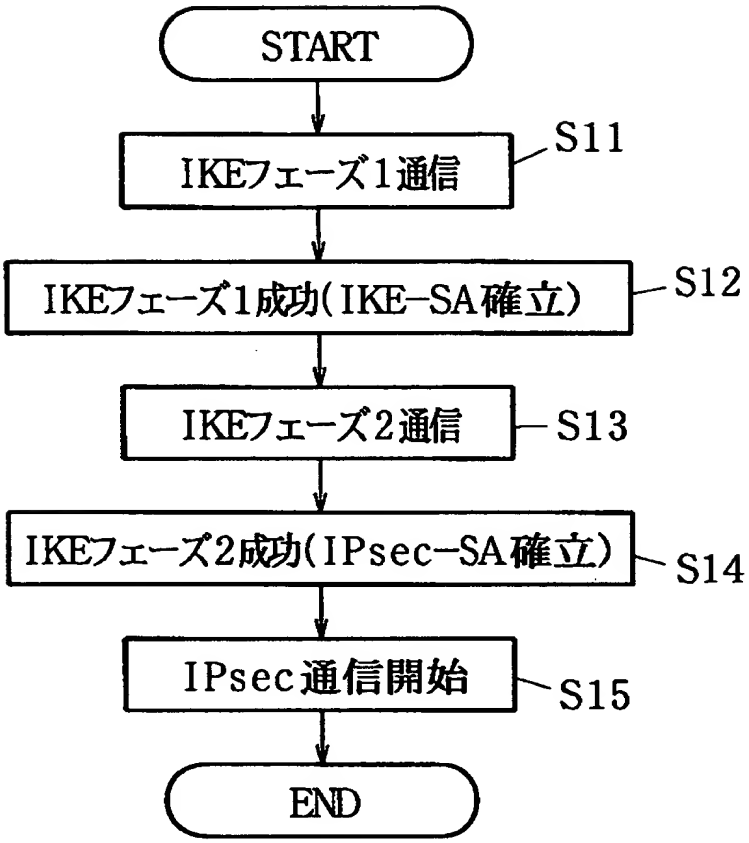
【図４】


101
108
WAN
102
セキュリティ・
ゲートウェイ
103
104
105
106
107

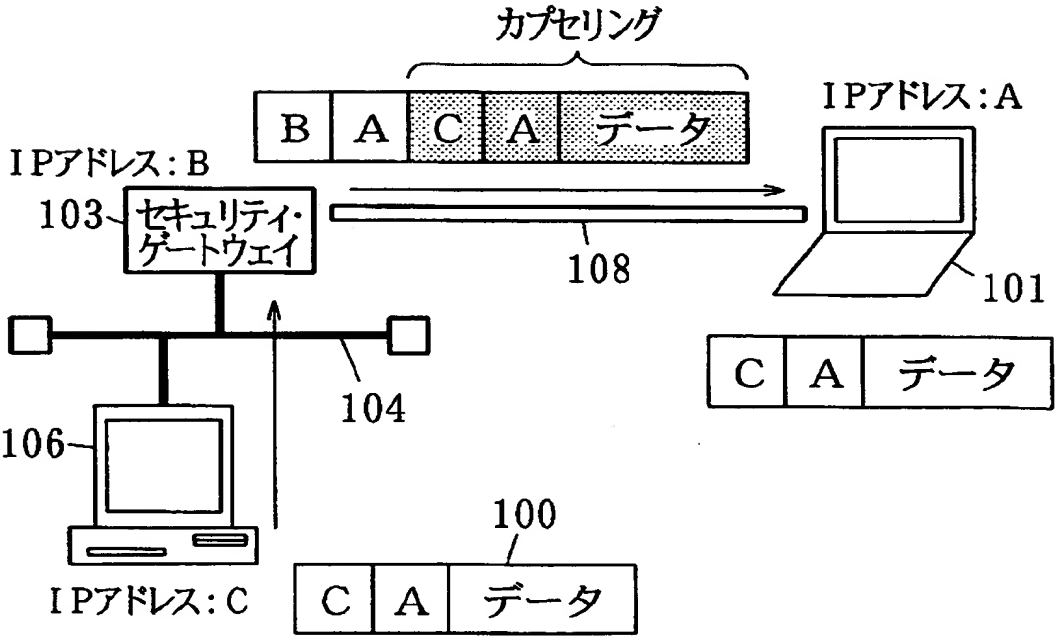
【図５】


WAN
103
102
101

【図６】


START
IKEフェーズ1通信
S11
IKEフェーズ1成功(IKE-SA確立)
S12
IKEフェーズ2通信
S13
IKEフェーズ2成功(IPsec-SA確立)
S14
IPsec通信開始
S15
END

【図７】


カプセリング
B
A
C
A
データ
IPアドレス:A
IPアドレス:B
103
セキュリティ・ゲートウェイ
108
101
C
A
データ
104
106
100
IPアドレス:C
C
A
データ

【書類名】　要約書

【要約】

【課題】　ＷＡＮを介して外部からアクセスするＰＣを仮想的にＬＡＮ配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるＶＰＮ通信方法を提供することを目的とする。

【解決手段】　公衆回線などから構成されるＷＡＮとＬＡＮ１０４との間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置１０３におけるＶＰＮ通信方法であって、ダイヤルアップ接続でＷＡＮに接続した外部のＰＣ１０１に対してＩＰｓｅｃプロトコルによりＶＰＮ１０８を実現する際、ＩＰｓｅｃ通信に先立つＩＫＥ通信時に、ＤＨＣＰ通信オプションをＩＫＥデータに統合し、トンネリングされたＩＰパケットにおけるＩＰｓｅｃ処理される送信元ＩＰアドレスＣの指定を実現する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
　〔変更理由〕　　新規登録
　　住　所　　大阪府門真市大字門真１００６番地
　　氏　名　　松下電器産業株式会社